WHAT IS CLAIMED IS:

1. A method comprising:
establishing an encrypted link between a peripheral device and a software component of an information handling system, wherein establishing the encrypted link includes generating a first seed key common to both the peripheral device and the software component;
providing the first seed key and a public encryption key associated with the peripheral device to a hardware controller; and
generating in the hardware controller, using the first seed key and the public encryption key, a second seed key different from the first seed key, the second seed key to encrypt communications between the software component and the hardware controller.

2. The method as in Claim 1, wherein generating the first seed key is performed by the software component.

3. The method as in Claim 2, wherein generating the first seed key includes:
using the public encryption key associated with the peripheral device to select a plurality of private encryption keys associated with the software component; and
determining the seed key based upon the selected private keys associated with the software component.

4. The method as in Claim 1, wherein generating the first seed key is performed by the peripheral device.

5. The method as in Claim 4, wherein generating the first seed key includes:

using the public encryption key associated with the software component to select from a plurality of private encryption keys associated with the peripheral device; and

summing the select private keys associated with the peripheral device.

6. The method as in Claim 1, wherein establishing an encrypted link includes performing orthogonal encryption of data transmitted to and from the hardware controller.

7. The method as in Claim 6, further including:

providing the public encryption key associated with the peripheral device and a private decryption key, associated with the software component, to the hardware component; and

providing public key encryption between the hardware controller and the peripheral device.

8. The method as in Claim 6, wherein the orthogonal encryption is performed using an orthogonal encryption key, wherein the orthogonal encryption key is capable of changing dynamically.

9. The method as in Claim 6, wherein the orthogonal encryption is performed using an orthogonal transform function, wherein the orthogonal transform function is capable of changing dynamically.

10. The method as in Claim 1, wherein the hardware controller is a video controller.1.

11. The method as in Claim 1, wherein the peripheral device is a display device.2.

12. The method as in Claim 1, wherein the step of establishing further includes the first seed key being based upon the peripheral device and the information handling system.

13. The method as in Claim 12, wherein the first seed key is unique to the peripheral device and the information handling system.3.

14. A hardware controller comprising:

a bus connection to receive a first seed key from a software component within an information handling system;

a digital communications connector to connect to a peripheral device and to receive a public encryption key from said peripheral device;

a first set of registers to store said first seed key, said first seed key common to both said information handling system and said peripheral device;

a second register to store said public encryption key; and

a processing circuit to generate, using said first seed key and said public encryption key,

a second seed key different from said first seed key, said second seed key to encrypt communications between said software component and said hardware controller.

15. The hardware controller as in Claim 14, wherein said information handling system generates said first key and wherein generation of said first key includes:

using said public encryption key to select a plurality of private encryption keys; and

combining said selected private encryption keys.

16. The hardware controller as in Claim 14, wherein communications between said hardware controller and said information handling system are performed over a system bus.

17. The hardware controller as in Claim 16, wherein said system bus is a Peripheral Component Interconnect bus.

18. The hardware controller as in Claim 14, wherein said digital communications connector is a Digital Video Interface connector.

19. The hardware controller as in Claim 14, wherein said hardware controller is a video controller.

20. The hardware controller as in Claim 14, wherein said peripheral device is a display device.

21. The hardware controller as in Claim 14, wherein encryption is performed using an orthogonal transform.

22. The hardware controller as in Claim 21, wherein the orthogonal transform is performed using an orthogonal encryption key, said orthogonal encryption key capable of changing dynamically.

23. The hardware controller as in Claim 21, wherein the orthogonal transform is performed using an orthogonal transform function, said orthogonal transform function capable of changing dynamically.

24. A system comprising:
a processor coupled to a system bus;
memory coupled to said system bus for use by said processor;
a collection of instructions to be stored in said memory and executed by said processor, said collection of instructions including instructions to establish an encrypted link between said system and a peripheral device, wherein establishing said encrypted link includes generating a first seed key common to both said peripheral device and said system, said collection of instructions further including instructions to deliver said first seed key to a peripheral controller; and
a peripheral controller including a bus connection to receive said first seed key;
a digital communications link to connect to said peripheral device and to receive a public encryption key from said peripheral device;
a first set of registers to store said first seed key;
a second register to store said public encryption key; and
a processing circuit to generate, using said first seed key and said public encryption key, a second seed key different from said first seed key, said second seed key to encrypt communications between said system and said peripheral controller.

25. The system as in Claim 24, wherein said memory includes random access memory and read-only memory.20.

26. The system as in Claim 24, wherein generating a first seed includes:
using said public encryption key to select a plurality of private encryption keys; and
combining said selected private encryption keys.

27. The system as in Claim 26, wherein said public encryption key and said plurality of private encryption keys are located in said memory.

28. The system as in Claim 24, wherein said system bus is a Peripheral Component Interconnect bus.

29. The system as in Claim 24, wherein said digital communications link is a Digital Video Interface connector.

30. The system as in Claim 24, wherein said peripheral controller is a video controller.

31. The system as in Claim 24, wherein said peripheral device is a display device.

32. The system as in Claim 24, wherein encryption is performed using an orthogonal transformation.

33. The system as in Claim 32, wherein the orthogonal transform is performed using an orthogonal encryption key, said orthogonal encryption key capable of changing dynamically.

34. The system as in Claim 32, wherein the orthogonal transform is performed using an orthogonal transform function, said orthogonal transform function capable of changing dynamically.

35. The system as in Claim 24, wherein the digital communications link is to receive a public encryption key from said peripheral device and to transmit encrypted digital data to said peripheral device.